

CLERK'S OFFICE**A TRUE COPY****Jan 21, 2021****s/ Daryl Olszewski****Deputy Clerk, U.S. District Court
Eastern District of Wisconsin****UNITED STATES DISTRICT COURT**

for the

Eastern District of Wisconsin

In the Matter of the Search of

(Briefly describe the property to be searched
or identify the person by name and address)834 N. 35th Street, Apartment 203, Milwaukee,
Wisconsin, more fully described in Attachment A

Case No. 21 MJ 45

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

See Attachment A

located in the Eastern District of Wisconsin, there is now concealed (identify the person or describe the property to be seized):

See Attachment B.

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- evidence of a crime;
- contraband, fruits of crime, or other items illegally possessed;
- property designed for use, intended for use, or used in committing a crime;
- a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

<i>Code Section</i>	<i>Offense Description</i>
21 U.S.C. § 841(a)(1)	Distribution of controlled substances

The application is based on these facts:

See attached Affidavit.

Continued on the attached sheet.

Delayed notice of _____ days (give exact ending date if more than 30 days): _____ is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.



Applicant's signature

Nesrodene Ghassoul, Task Force Office

Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by
telephone _____ (specify reliable electronic means).

Date: January 21, 2021


Judge's signature

William E. Duffin

Printed name and title

**AFFIDAVIT IN SUPPORT OF CRIMINAL COMPLAINT
AND SEARCH WARRANT**

I, Nesrodene Ghassoul, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for (1) a criminal complaint and arrest warrant for **Curlee J. ASHFORD** (DOB: XX/XX/1966); and (2) a warrant, pursuant to Rule 41 of the Federal Rules of Criminal Procedure, to search the premises known as **834 N. 35th Street, Apartment 203, Milwaukee, Wisconsin**, hereinafter “**PREMISES**,” further described in Attachment A, for the things described in Attachment B.

2. I am a Police Officer with the Milwaukee Police Department and have been since July of 2015. As of December of 2019, I've been assigned and attached as a Federally Deputized Task Force Officer (TFO) with the Southeastern Wisconsin Regional Gang Task Force. Prior to being assigned as a Task Force Officer, I was assigned to the Milwaukee Police Department, District 7 Anti-Gang Unit from June 2018 until December 2019. I am an investigator or law enforcement officer of the United States within the meaning of 18 U.S.C. Section 2510(7), in that I am empowered by the law to conduct investigations of and to make arrests for federal felony arrests.

3. As a law enforcement and Task Force Officer, I have had formal training in the investigation of drug trafficking. I have also participated in the investigation of narcotics-related offenses, which have resulted in the prosecution and conviction of individuals and the seizure of illegal drugs, weapons, United States currency, and other evidence of criminal activity. Additionally, I have spoken with other experienced narcotics investigators on numerous occasions concerning the method and practices of drug traffickers and money launderers. Through my training and experience, I have become aware of the methods used by drug traffickers to manufacture, smuggle, safeguard, and distribute narcotics, and to collect and launder trafficking-derived proceeds. I am also familiar with the actions, habits, traits, methods, and terminology used by drug traffickers and abusers of controlled substances. More specifically, I am familiar with the street names of various drugs, including marijuana, heroin, cocaine, cocaine base, and methamphetamine. I am familiar with methods that are commonly used by drug dealers to package and prepare controlled substances for sale in the State of Wisconsin and elsewhere.

4. As a narcotics investigator, I have participated in all aspects of drug investigations, including physical surveillance, execution of search warrants, undercover operations, analysis of phones, and the arrests of numerous drug

traffickers. I have worked with numerous informants in the investigation of drug trafficking in the State of Wisconsin. I have directed informants during controlled buys of controlled substances, performed undercover meetings with individuals, and made monetary payments to drug traffickers for past controlled substances received. I have participated in the execution of numerous state and federal search warrants in which controlled substances, drug paraphernalia, drug proceeds, drug-related records, financial records, and electronic devices with data were seized. I know that drug traffickers commonly have in their possession, and at their residences and other locations where they exercise dominion and control, firearms, ammunition, and records or receipts pertaining to such. I have interviewed many individuals involved in drug trafficking and have obtained information from them regarding acquisition, sale, importation, manufacture, and distribution of controlled substances.

5. In the course of my employment and experience, I have also become aware of techniques and practices used by narcotics traffickers to avoid detection by law enforcement. Examples of those techniques include the use of multiple locations to conduct narcotics related activities, the use of counter-surveillance, the use of hidden compartments in vehicles to conceal narcotics and currency, the use of mobile telephones, voice mail, texting, instant messaging, email, the

compartmentalized use of multiple telephones, and the use of numerous associates and "workers" to further their criminal organization. I have also become aware of the various techniques individuals use to conceal the source or nature of drug proceeds. Examples of those techniques include the purchase of assets and financial instruments in nominee names using cash and "structuring" transactions to avoid certain reporting requirements of financial institutions.

6. Based upon my training and experience, I know that computer hardware and software may be important to a criminal investigation in two distinct and important respects: (1) the objects themselves may be instrumentalities, fruits, or evidence of crime, and/or (2) the objects may have been used to collect and store information about crimes (in the form of electronic data). Rule 41 of the Federal Rules of Criminal Procedure permits the government to search and seize computer hardware and software which are (1) instrumentalities, fruits, or evidence of crime, or (2) storage devices for information about crime.

7. To this end, based upon my training and experience, I know that individuals involved in drug trafficking frequently use cellular telephones to maintain contact and arrange transactions with their sources and customers of and co-conspirators in the distribution of controlled substances. I have also found it very common for crime suspects to use their cellular telephones to communicate aurally

or via electronic message in "text" format with individuals whom they purchase, trade, or otherwise negotiate to obtain illegal drugs. I also believe that it is common for crime suspects who possess illegal controlled substances and firearms to often take or cause to be taken photographs and other visual depictions of themselves, their associates, and the illegal controlled substances and firearms that they control, possess, buy, and sell.

8. The facts in this affidavit come my personal observations, my training and experience, my review of oral and written reports of other law enforcement officers participating in this and related investigations, records, documents, and other evidence obtained during this investigation. The investigation to date has involved traditional law enforcement methods, including, but not limited to confidential informants, interviews, documentary evidence, phone analysis, and physical surveillance.

9. This affidavit is intended to show merely that there is probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

PROBABLE CAUSE

10. The United States, including the FBI and the FBI's Southeastern Wisconsin Regional Gang Task Force, are conducting a criminal investigation of

Curlee J. ASHFORD (DOB: XX/XX/1966) regarding possible violations of Title 21, United States Code, Section 841(a)(1) (distribution of and possession with intent to distribute controlled substances).

11. In October of 2019, case agents interviewed a confidential source (CS #1). CS #1 stated “**BUG**” is a Gangster Disciple gang member with ties to Chicago, Illinois. CS #1 indicated “**BUG**” sells heroin from his apartment, which is located at 834 N. 35th Street Apt. 203, Milwaukee, Wisconsin, **PREMISES**. Additionally, CS #1 stated “**BUG**” holds at least 100 grams of heroin at a time. CS #1 advised case agents that they could make a controlled buy of heroin from “**BUG**.”

12. On October 18, 2019, case agent showed a single Milwaukee Police Department booking photograph of **Curlee J. ASHFORD** (DOB: XX/XX/1966) to CS #1. The photograph was unlabeled and contained no identifying information. CS #1 positively identified the photograph as the person CS #1 knew as “**BUG**.”

13. Case agents believe CS #1 is reliable and credible. First, CS #1 has provided information since October 2019. Second, CS #1’s information is consistent with case agent’s knowledge of violent gang subjects in Milwaukee, Wisconsin. Furthermore, substantial portions of CS #1’s information has been corroborated by controlled drug purchases, money deliveries, and consensually recorded phone calls with **ASHFORD**, as well as through independent investigation, including

surveillance and information from other sources. CS #1 is a convicted felon with prior obstruction, carrying a concealed weapon, and possession and distribution of narcotics convictions. In relation to CS #1's most recent narcotics conviction, the sentencing court was advised of CS #1's cooperation in the **ASHFORD** investigation through the date of sentencing. CS #1 is also receiving monetary compensation for his cooperation with law enforcement. For these reasons, case agents believe CS #1 to be reliable.

14. On December 18, 2019, case agents interviewed CS #1. CS #1 stated CS #1 bought heroin from “**BUG**” between thirty-seven to forty times over the last five years. CS #1 stated CS #1 purchased approximately twenty-five to fifty grams of heroin each time. In addition, CS #1 stated CS #1 purchased larger quantities, over 100 grams, of heroin on two occasions. Additionally, CS #1 stated “**BUG**” keeps the heroin in the oven of his apartment and has seen guns in “**BUG’s**” apartment. According to CS #1, “**BUG**” obtains his heroin from a Chicago area supplier. CS #1 provided phone numbers of (773) 569-9645, or Target Cell Phone #1, (312) 568-6998, or Target Cell Phone #2, and (414) 629-5943, or Target Cell Phone #3, for “**BUG**.”

January 9, 2020, Controlled Purchase of Heroin and Fentanyl

15. Based upon my training and experience, I know that a “controlled buy” (and/or controlled contact) is a law enforcement operation in which a confidential source purchases drugs from a target. The operation is conducted using surveillance, usually audio and video taping equipment, and pre-recorded purchase money. When a confidential source is used, s/he is searched for contraband, weapons, and money before the operation. The confidential source is also wired with a concealed body recorder and monitoring device. When the transaction is completed, the confidential source meets cases agents at a pre-determined meet location and gives the purchased drugs and the recording/monitoring equipment to the case agents. The confidential source is again searched for contraband, weapons, and money. A sample of the suspected drugs is then field tested by case agents for the presence of controlled substance and then placed in inventory pursuant to normal inventory procedures. Telephone calls to the target by the confidential source are consensually recorded calls under the direction and control of case agents and made in the presence of case agents.

16. On January 9, 2020, case agents used CS #1 to conduct a controlled purchase of heroin from “BUG.” CS #1 made a consensually recorded phone call to Target Cell Phone #1. “BUG” answered the phone and CS #1 and “BUG” discussed

meeting. “BUG” stated he would be ready in twenty minutes. Next, case agents provided CS #1 with a recording device and a total of \$1,000 pre-recorded money for the controlled purchase, and then established surveillance in the meet location of 2100 N. 34th Street, Milwaukee, Wisconsin. CS #1 drove to and parked in the alley of 2100 N. 34th Street, Milwaukee, Wisconsin. Surveillance observed a two-toned silver and blue older Ford pickup truck pull into the alley and park behind CS #1’s vehicle. CS #1 exited the vehicle and walked to the driver side door of the Ford pickup truck, where CS #1 remained for only a short period of time. CS #1 got back into CS #1’s vehicle and drove off. Surveillance observed the Ford pickup truck remain at the location and identified an additional suspected drug transaction take place with another individual at the front passenger door of the Ford pickup truck. Case agents believe “BUG” sold narcotics to the other individual.

17. After the transaction, case agents met with CS #1 and seized the heroin and the recording device. CS #1 also provided the case agents with \$20 from the drug purchase as CS #1 had calculated the amount of narcotics should only cost \$980, not \$1,000. Case agents field tested the heroin with positive results for heroin and fentanyl and weighed approximately 15.09 grams.

18. After the controlled purchase, CS #1 was briefed. CS #1 stated CS #1 parked in the alley in the area of 2100 N 34th Street, Milwaukee, Wisconsin and

waited for “BUG.” CS #1 contacted “BUG” over the phone as “BUG” was taking a long time to arrive. While waiting for “BUG,” CS #1 stated another individual arrived in the alley as “BUG” pulled up in his truck. CS #1 got out of CS #1’s vehicle and walked to the driver’s side door of “BUG’s” truck. CS #1 gave \$980 in pre-recorded law enforcement funds to “BUG.” In exchange, “BUG” gave CS #1 the narcotics. CS #1 stated “BUG” kept the narcotics on his lap.

19. Case agents reviewed the recording from the recording device used by CS #1 to confirm CS #1’s purchase of heroin on January 9, 2020 from **ASHFORD**.

20. On January 9, 2020, a case agent showed a single Milwaukee Police Department booking photograph of **Curlee J. ASHFORD** (DOB: XX/XX/1966) to CS #1. The photograph was unlabeled and contained no identifying information. CS #1 positively identified the photograph as the person CS #1 knew as “BUG” and the person that sold CS #1 the heroin on January 9, 2020.

January 22, 2020, Controlled Purchase of Heroin and Fentanyl

21. On January 22, 2020, case agents used CS #1 to conduct a controlled purchase of heroin from “BUG.” CS #1 made a consensually recorded phone call to the Target Cell Phone #2. “BUG” answered the phone and “BUG” and CS #1 discussed meeting at “BUG’s” place, the **PREMISES**. CS #1 told “BUG” to meet at a different location and they both agreed. Shortly after the terminated call, CS #1

made another phone call to the Target Cell Phone #2 and informed “BUG” CS #1 would meet at the **PREMISES** instead. Next, case agents provided CS #1 with a recording device and pre-recorded money for the controlled purchase and then established surveillance in the area. CS #1 drove, while being followed by case agents, to the **PREMISES**. Surveillance observed CS #1 make a U-turn and park south of the address of the **PREMISES**. CS #1 exited the vehicle and walked to the exterior of the apartment complex containing the **PREMISES**. CS #1 waited outside the entry door for a short time before CS #1 was let in the front door. After approximately seven minutes, surveillance observed CS #1 exit the entry door to the complex containing the **PREMISES**, walk to CS #1’s vehicle, and leave the location. Surveillance followed CS #1 to the meet location. At the meet location, the case agents met with CS #1 and seized the heroin and the recording device. Case agents field tested the heroin with positive results for opiates and fentanyl and weighed approximately 45.49 grams.

22. After the controlled purchase, CS #1 was briefed. CS #1 stated CS #1 drove to the **PREMISES**, parked, and walked to the main entry. CS #1 called “BUG” to let CS #1 into the building. “BUG” came to the door and let CS #1 in. CS #1 stated they took the elevator up to the **PREMISES**. “BUG” provided CS #1 with

the prepackaged narcotics, and in exchange, CS #1 provided “**BUG**” with the money. CS #1 then left the **PREMISES**, got in the vehicle, and drove to the meet spot.

23. Case agents reviewed the recording from the recording device used by CS #1 to confirm CS #1’s purchase of heroin on January 22, 2020, from **ASHFORD**.

24. On or about April 4, 2020, CS #1 reported to law enforcement that **ASHFORD** had trouble with his previous source of narcotics supply and had ceased all communications with this source. **ASHFORD** reportedly obtained a new source of supply for narcotics in Chicago and asked CS #1 to go to Chicago and pick up a resupply of narcotics from the new supplier.

25. According to CS #1, **ASHFORD** temporarily relocated to Chicago during the summer and fall of 2020. CS #1 stated that **ASHFORD** returned back to Milwaukee, Wisconsin, around November 2020, and has resumed narcotics trafficking.

January 13, 2021, Controlled Purchase of Heroin and Fentanyl

26. On January 13, 2021, case agents used CS #1 to conduct a controlled purchase of heroin from “**BUG**.” CS #1 made a consensually recorded phone call to the Target Cell Phone #3. “**BUG**” answered the phone and discussed meeting with CS #1. “**BUG**” told CS #1 that he is home and to meet him at this residence where the narcotics would be ready. CS #1 told “**BUG**” CS #1 is on the way and terminated

the phone call. Case agents provided CS #1 with a recording device and \$1,300 in pre-recorded money for the controlled purchase. CS #1 then entered CS #1's vehicle and drove, while being followed by case agents, to the **PREMISES**.

27. Surveillance observed CS #1 park on the east side of the block near the address of 834 N 35th Street. CS#1 then exited the vehicle, approached the exterior of the building, and entered the vestibule of the building. Approximately ten minutes later, surveillance observed CS #1 exit the entry door of the building containing the **PREMISES**. CS #1 then walked to CS #1's vehicle and drove away to the pre-determined meet location, while being followed by case agents. At the meet location, the case agents met with CS#1 and seized the heroin and recording device. Case agents field tested the heroin with positive results for opiates and fentanyl and had a total weight 15 grams.

28. After the controlled purchase, CS #1 was briefed. CS #1 stated CS #1 drove to the **PREMISES**, parked in front of the residence containing the **PREMISES**, and called "BUG" to let CS #1 inside the building. An unknown black male met CS #1 at the door and let CS #1 inside the building. The unknown black male then took CS #1 directly to the **PREMISES**. CS #1 entered the **PRESMISES** and provided "BUG," who was sitting inside the kitchen, with the \$1,300 in pre-

recorded bills and received, in exchange for the currency, a clear bag containing the narcotics. CS #1 then left the **PREMISES** and walked into CS #1's vehicle.

29. Case agents reviewed the recording from the recording device used by CS #1 to confirm CS #1's purchase of heroin on January 13, 2021, from **ASHFORD**. **ASHFORD** is heard on the recording stating that he "got some shit way better than that too," and that he "went down there and bought all that dope." **ASHFORD** further states "he said he's gonna get some more and call me," as well as "I want it all, whatever he has I'll buy." Based on my training, experience, and familiarity with this investigation, I believe that **ASHFORD** stated that he had different kinds of heroin, and that he was planning on buying more narcotics from his source of supply.

PREMISES Information

30. The address of 834 N 35th Street Milwaukee, Wisconsin, is a multi-unit apartment complex currently owned by Clare Towers, INC. Utility records for the **PREMISES** are in the name of **Curlee ASHFORD** and have been active since August 1, 2017. A Wisconsin Department of Transportation query revealed that **Curlee ASHFORD** has listed the **PREMISES** as his current address since September 17, 2017.

TECHNICAL TERMS

31. Based on my training and experience, I use the following technical terms to convey the following meanings:

- a. IP Address: The Internet Protocol address (or simply “IP address”) is a unique numeric address used by computers on the Internet. An IP address looks like a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

- b. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

c. Storage medium: A storage medium is any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS

41. As described above and in Attachment B, this application seeks permission to search for records that might be found on the **PREMISES**, in whatever form they are found. One form in which the records might be found is data stored on a computer's hard drive, cellular telephone, or other storage media. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

42. *Probable cause.* I submit that if a computer, cellular telephone, or storage medium is found on the **PREMISES**, there is probable cause to believe those records will be stored on that computer or storage medium, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at

little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person “deletes” a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer’s operating system may also keep a record of deleted data in a “swap” or “recovery” file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers’ internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory “swap” or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or “cache.”

43. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium in the **PREMISES** because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record

information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

b. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the “who, what, why, when, where, and how” of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculpating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that logs computer user account session times and durations, computer activity associated with user

accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculpate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g.,

running a “wiping” program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the

presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

f. I know that when an individual uses a computer to operate a website that is used for illegal conduct, the individual's computer will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The computer is an instrumentality of the crime because it is used as a means of committing the criminal offense. The computer is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that a computer used to commit a crime of this type may contain: data that is evidence of how the computer was used; data that was sent or received; notes as to how the criminal conduct was achieved; records of Internet discussions about the crime; and other records that indicate the nature of the offense.

44. *Necessity of seizing or copying entire computers or storage media.* In most cases, a thorough search of a premises for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the

computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

a. The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

b. Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before

a search what tools or knowledge will be required to analyze the system and its data on the Premises. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

c. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

45. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

46. Because other people may share the **PREMISES** as a residence, it is possible that the **PREMISES** will contain storage media that are predominantly used, and perhaps owned, by persons who are not suspected of a crime. If it is nonetheless determined that that it is possible that the things described in this

warrant could be found on any of those computers or storage media, the warrant applied for would permit the seizure and review of those items as well.

47. Unlocking Apple brand devices: I know based on my training and experience, as well as from information found in publicly available materials including those published by Apple, that Apple devices are used by many people in the United States, and that some models of Apple devices such as iPhones and iPads offer their users the ability to unlock the device via the use of a fingerprint or thumbprint (collectively, “fingerprint”) in lieu of a numeric or alphanumeric passcode or password. This feature is called Touch ID.

a. If a user enables Touch ID on a given Apple device, he or she can register up to 5 fingerprints that can be used to unlock that device. The user can then use any of the registered fingerprints to unlock the device by pressing the relevant finger(s) to the device’s Touch ID sensor, which is found in the round button (often referred to as the “home” button) at the bottom center of the front of the device. In my training and experience, users of Apple devices that offer Touch ID often enable it because it is considered to be a more convenient way to unlock the device than by entering a numeric or alphanumeric passcode or password, as well as a more secure way to protect the device’s contents. This is particularly true when

the user(s) of the device are engaged in criminal activities and thus have a heightened concern about securing the contents of the device.

b. In some circumstances, a fingerprint cannot be used to unlock a device that has Touch ID enabled, and a passcode or password must be used instead. These circumstances include: (1) when more than 48 hours has passed since the last time the device was unlocked and (2) when the device has not been unlocked via Touch ID in 8 hours and the passcode or password has not been entered in the last 6 days. Thus, in the event law enforcement encounters a locked Apple device, the opportunity to unlock the device via Touch ID exists only for a short time. Touch ID also will not work to unlock the device if (1) the device has been turned off or restarted; (2) the device has received a remote lock command; and (3) five unsuccessful attempts to unlock the device via Touch ID are made.

c. If Touch ID enabled Apple devices are found during a search of the **PREMISES**, the passcode or password that would unlock such the devices are presently unknown to law enforcement. Thus, it will likely be necessary to press the finger(s) of the user(s) of any Apple device(s) found during the search of the **PREMISES** to the device's Touch ID sensor in an attempt to unlock the device for the purpose of executing the search authorized by this warrant. Attempting to unlock the relevant Apple device(s) via Touch ID with the use of the fingerprints of

the user(s) is necessary because the government may not otherwise be able to access the data contained on those devices for the purpose of executing the search authorized by this warrant.

d. In my training and experience, the person who is in possession of a device or has the device among his or her belongings at the time the device is found is likely a user of the device. However, in my training and experience, that person may not be the only user of the device whose fingerprints are among those that will unlock the device via Touch ID, and it is also possible that the person in whose possession the device is found is not actually a user of that device at all. Furthermore, in my training and experience, I know that in some cases it may not be possible to know with certainty who is the user of a given device, such as if the device is found in a common area of a premises without any identifying information on the exterior of the device. Thus, it will likely be necessary for law enforcement to have the ability to require **ASHFORD** to press his finger(s) against the Touch ID sensor of the locked Apple device(s) found during the search of the **PREMISES** in order to attempt to identify the device's user(s) and unlock the device(s) via Touch ID.

e. Although I do not know which of a given user's 10 fingerprints is capable of unlocking a particular device, based on my training and experience I

know that it is common for a user to unlock a Touch ID-enabled Apple device via the fingerprints on thumbs or index fingers. In the event that law enforcement is unable to unlock the Apple device(s) found in the **PREMISES** as described above within the five attempts permitted by Touch ID, this will simply result in the device requiring the entry of a password or passcode before it can be unlocked.

48. Due to the foregoing, I request that the Court authorize law enforcement to press **ASHFORD's** fingers (including thumbs) to the Touch ID sensor of the Apple brand device(s), such as an iPhone or iPad, found at the **PREMISES** for the purpose of attempting to unlock the device via Touch ID in order to search the contents as authorized by this warrant.

CONCLUSION

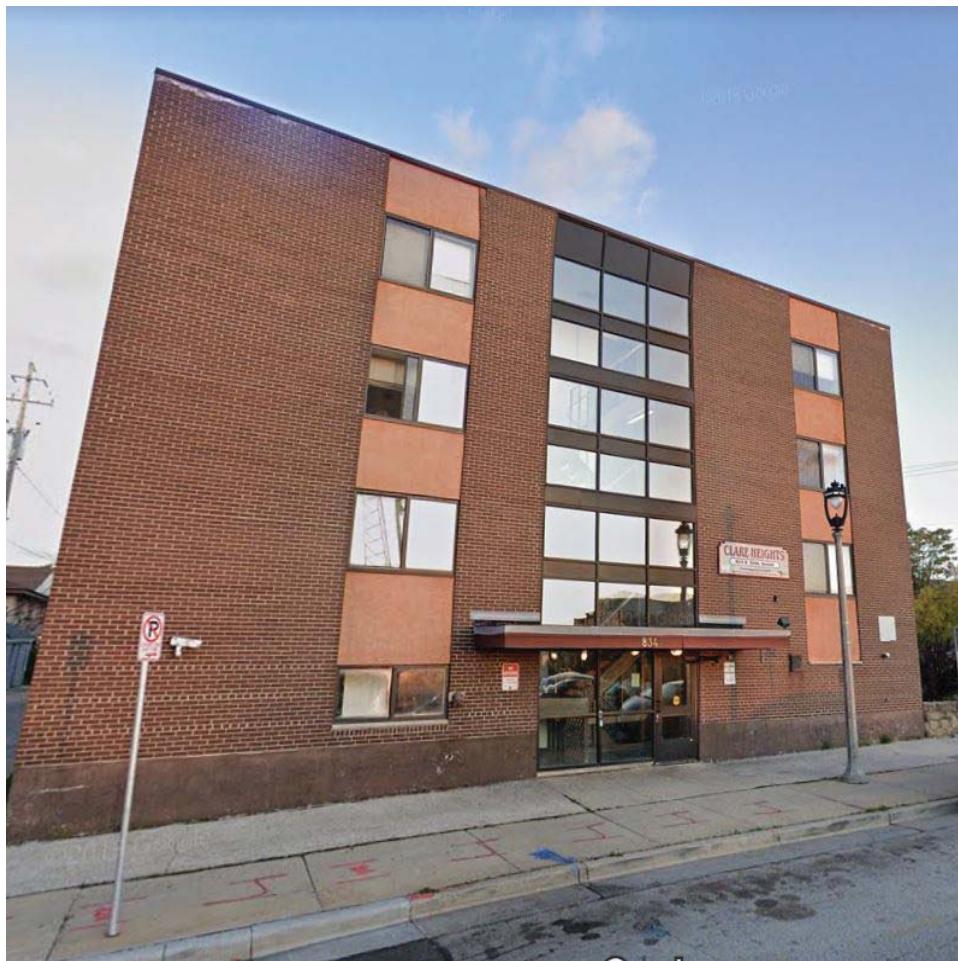
49. Based on the facts contained within this affidavit, I believe there is probable cause to believe that **Curlee J. ASHFORD** committed the crimes of distribution of controlled substances, in violation of Title 21, United States Code, Sections 841(a)(1) and 841(b)(1)(B).

50. Based upon the facts contained within this affidavit, I believe there is probable cause for a warrant to search the **PREMISES** described in Attachment A and seize the items described in Attachment B.

ATTACHMENT A

Property to be searched

834 N. 35th Street, Apartment 203, Milwaukee, Wisconsin. This property is used by **Curlee J. ASHFORD**. This address is further described as a multi-colored three-story apartment building with underground parking. The front half of the apartment building has brown brick with white trim separated by light brown panels between residential windows. The latter half of the building is primarily light-tan in color with windows surrounded by black trim. An awning bearing the numbers "834" in white lettering is affixed above the front entrance door. To the right of the awning a sign with "Clare Heights" is affixed to the brick that also displays the address of "834 N. 35th Street." Apartment 203 located on the second floor on the south side of the building.



ATTACHMENT B

Property to be seized

1. Evidence, fruits, and instrumentalities of violations of Title 21, United States Code, Section 841(a)(1) (Distribution of and possession with intent to distribute controlled substances), those violations involving Curlee J. ASHFORD, including:

- a. Controlled substances, controlled substance analogues, or listed chemicals;
- b. Paraphernalia associated with the manufacture and distribution of controlled substances including but not limited to materials and items used for packaging, processing, diluting, weighing, and distributing controlled substances, such as scales, funnels, sifters, grinders, glass panes and mirrors, razor blades, plastic bags, and heat-sealing devices;
- c. Duffel, canvas bags, suitcases, safes, or other containers to hold or transport controlled substances and drug trafficking related items and proceeds;
- d. Proceeds of drug trafficking activities, such as United States currency, precious metals, financial instruments, and jewelry, and documents and deeds reflecting the purchase or lease of real estate, vehicles, precious metals, jewelry or other items obtained with the proceeds from drug trafficking activities;
- e. Firearms, ammunition, magazines, gun boxes, firearm purchase records or receipts, and other paraphernalia associated with firearms;
- f. Bank account records, loan documents, wire transfer records, money order receipts, postal express mail envelopes, bank statements, safe deposit box keys and records, money containers, financial records and notes showing payment, receipt, concealment, transfer, or movement of

money generated from the sale of controlled substances, or financial transactions related to the trafficking of controlled substances;

- g. Drug or money ledgers, drug distribution or customer lists, drug supplier lists, correspondence, notations, logs, receipts, journals, books, records, and other documents noting the price, quantity, and/or times when controlled substances were obtained, transferred, sold, distributed, and/or concealed;
- h. Personal telephone books, address books, telephone bills, photographs, letters, cables, telegrams, facsimiles, personal notes, receipts, documents and other items or lists reflecting names, addresses, purchases, telephone numbers, addresses and communications regarding illegal activities among and between members and associates involved in drug trafficking activities;
- i. Records of off-site storage locations, including but not limited to safe deposit box keys and records, and records and receipts and rental agreements for storage facilities;
- j. Cellular telephones, Smartphones, text messaging systems, and other communication devices, and all electronic storage areas on the device including stored telephone numbers, recently called numbers list, text messages, digital audio and/or video recordings, pictures, settings, and any other user defined settings and/or data, as well as any records associated with such communications services used to commit drug trafficking offenses;
- k. Records, items and documents reflecting travel for the purpose of participating in drug trafficking activities, such as passports, airline tickets, bus tickets, vehicle rental receipts, credit card receipts, taxi cab receipts, hotel and restaurant receipts, canceled checks, maps, and records of long distance calls reflecting travel;
- l. Indicia of occupancy, residency or ownership of the premises and things described in the warrant, including utility bills, telephone bills, loan payment receipts, rent receipts, trust deeds, lease or rental agreements, addressed envelopes, escrow documents and keys;
- m. Photographs, videotapes or other depictions of assets, firearms, coconspirators, or controlled substances; and

2. Computers, cellular telephones, or storage media used as a means to commit the violations described above;
3. For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER"):
 - a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;
 - b. evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to crime under investigation and to the computer user;
 - c. evidence indicating the computer user's state of mind as it relates to the crime under investigation;
 - d. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;
 - e. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;
 - f. evidence of the times the COMPUTER was used;
 - g. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;
 - h. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;

- i. records of or information about Internet Protocol addresses used by the COMPUTER;
- j. records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;
- k. contextual information necessary to understand the evidence described in this attachment.

As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term "storage medium" includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

This warrant authorizes law enforcement to press **ASHFORD's** fingers (including thumbs) to the Touch ID sensor of the Apple brand device(s), such as an

iPhone or iPad, found at the **PREMISES** for the purpose of attempting to unlock the device via Touch ID in order to search the contents as authorized by this warrant.

This warrant also authorizes a review of electronic storage media and electronically stored information seized or copied pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.